REMARKS

Claims 1–69 are pending and remain rejected. Claims 1–12, 19–21, 24, 27, 33–39, 45–47, 50, 53, 59–61 and 64–69 remain rejected under 35 U.S.C. § 102(b) based on *Fisherman, et al.* (U.S. Patent No. 5,586,301). Claims 13–17, 28–32, 40–44, 54–58 are rejected under 35 U.S.C. § 103(a) based on *Fisherman* in view of Glossary of Information Technology Acronyms and Terms ("GITAT"). For the reasons set forth below, the Applicant respectfully traverses the rejections of the pending claims and requests reconsideration.

Amendments to the Claims

New claims 70, 71, 72 and 73 include elements previously not claimed but are supported as follows:

Claim 70 is supported at least in the specification on page 14, line 28 through page 15, line 3.

Claim 71 is supported at least in the specification on page 5, line 25 through page 6, line 22, page 11, lines 1-4, page 16, lines 24–28.

Claim 72 is supported at least in the specification on page 6, lines 2–6.

Claim 73 is supported at least in the specification on page 6 lines 16–20.

Further, support for the new claims may be found in the original claims as well.

Fisherman

Fisherman is directed to a personal computer hard disk protection system (*Fisherman*, Title). The hard disk has a logical structure, including an operating system having logical drives. (*Fisherman*, Col. 2, lines 32–35). The system comprises protection programs that interpret the logical drives as a fixed set of zones on the hard disk for a particular user and wherein each of the fixed set of zones each has respective access rules. (*Fisherman*, Col. 2, lines 35–38). The

system also includes a hardware module responsive to the protection programs that either allows or denies access to the hard disk based on the access rules. (*Fisherman*, Col. 2, lines 38–41).

Claims Rejected – 35 U.S.C. § 102

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single reference.[1] Additionally, the single reference must set forth each of the claim elements as arranged by the claims.[2]

Independent Claim 1

Claim 1 recites:

1. (Original) A method for protection of computer assets from unauthorized access comprising the steps of:

receiving in a protection engine, an interface control command;

determining whether the interface control command introduces a security risk;

when the interface control command introduces a security risk, determining a state of a switch; then the state of the switch is a protected state, inhibiting execution of the interface control command; and

when the state of the switch is in an unprotected state, allowing execution of the interface control command.

According to the Office Action "*Fisherman* clearly teaches receiving a control-command handler, which obviously receives control commands to handle" (Col. 4, lines 2—3). However,

---

[1] Glaverzel Societe Anonyme v. Northlake Marketing & Supply, Inc., 75 F.3d 1550, 1554 (Fed. Cir. 1999); Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1953 (Fed. Cir. 1987); *see* MPEP 2131.

[2] Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *see* MPEP 2131.

the cited portion of *Fisherman* that states "the set of protection programs includes a protection initialization program 44, a disk-request handler 46, a control-command handler 48, a protection control program 50, and a set of key programs..." merely describes a control-command handler rather than "receiving any protection engine, an interface control command." The Applicant would like to point out that the claims require that the protection engine receives "an interface control command." Applicant would like to point out the distinction between a protection engine receiving "an interface control-command" as claimed and merely describing a control-command handler as cited in *Fisherman*. As a result, the Office Action continues to ignore elements of the claims, mainly "an interface control command." Further, the cited portion of *Fisherman* fails to describe an interface control command as claimed.

The *Fisherman* language cited by the final Office Action on page 2, reference number 2 states "a personal computer hard disk protection system (HDPS) that comprises a hardware module, 22 known as the protection-program support module (PPSM), and protection software 24" (*Fisherman* Col. 3, lines 33–36) merely describes generally a protection-program support module (PPSM) and protection software 24 rather than "receiving in a protection engine, an interface control command." Applicant would like to point out the distinction between a protection-program support module and protection software 24 and "receiving in a protection engine, an interface control command." Applicant submits that the cited portion of *Fisherman* does not recite any type of command, let alone "an interface control command." As a result, the Office Action has mischaracterized *Fisherman* and ignored a element of the claims. For at least these reasons, the Office Action fails to establish where *Fisherman* as cited recites, and a showing is requested of among other things, "receiving in a protection engine, an interface control command." Therefore, the Office Action fails to establish how *Fisherman* anticipates

Claim 1. Further, Applicant requests a showing of where *Fisherman* teaches "receiving in a protection engine, an interface control command."

According to the final Office Action:

> Security risks as taught by [SIC] are commands that can cause potential damage to the system. These commands must only be executed from authorized program entities. Examiner relies on the specification of *Fisherman* in columns 5-7 for support of this interpretation. The system must be able to recognize individual commands if it is able to differentiate between potentially threatening commands and lesser important commands.

The Office Action cites to paragraphs 5-7 of *Fisherman*, three columns in *Fisherman* for describing "a security risk." According to 37 C.F.R. §1.104(c)(2): In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his/her command. When a reference is complex or shows or describes inventions other than that claimed by the Applicant, the particular part relied on must be designated as merely as practicable. The pertinence of each reference, if not apparent, must be clearly explained in each rejective claim specified. The Applicant requests a showing of "determining whether the interface control command introduces a security risk."

The Office Action appears (on page 10) to cite to Col. 4, lines 23—30 and Col. 5, lines 7—11. As previously stated, Applicant could not find where in Col. 4, lines 23—30 *Fisherman* describes "determining whether the interface control command introduces a security risk."

For example, the *Fisherman* language cited in the Office Action that states "during the protection process each logical drive of the MS-DOS Operating System 28 is interpreted by the HDPS 20 as a fixed set of zones of the disk space, with different access rules for each zone" (*Fisherman*, Col. 5, lines 7–11) is limited to interpreting each logical drive of the MS-DOS Operating System 28 as a fixed set of zones of the disk space, with different access rules for each zone, rather than "determining whether the interface control command introduces a security

risk." Applicant would like to point out the distinction between a logical drive of the MS-DOS Operating System 28 interpreted as a fixed set of zones of the disk space and "determining whether the interface control command introduces a security risk." Applicant cannot find where *Fisherman*, as cited, describes a security risk, let alone "determining whether the interface control command introduces a security risk." As such, the Office Action has yet again ignored a element of the claims. Accordingly, a corresponding showing is requested. As such, for at least these reasons, the Office Action fails to show how *Fisherman* anticipates the claims.

The *Fisherman* language cited by the Office Action that states "In the passage mode, the PPSM 22 permits the protection programs to be read, and does not affect the access to the hard disk 34 by the CPU 64," "In order to obtain free access to the hard disk 34, the CPU 64 must switch the PPSM 22 to the passive mode and to do this, the CPU 64 must use one of the key programs" and "the reason for the use of the key program is that the PPSM 22 determines the type of program that is attempting to change the status, and the PPSM 22 allows a change in the status only if flags are present indicating that the key program is active" is limited to determining the type of program which is attempting to change the status, and the PPSM allows a change in its status only if flags are present indicating that the key program is active rather than "when the interface control command introduces a security risk, determining a state of a switch." Applicant would like to point out the distinction between the PPSM determining the type of program that is attempting to change its status and allowing a change in its status only if flags are present indicating that the key program is active rather than "when the interface control command introduces a security risk, determining a state of a switch." The cited portion of the Office Action fails to describe an interface control command and a security risks let alone "when the interface control command introduces a security risk." Further, the cited portion of *Fisherman*

fails to describe a switch, let alone "determining a state of a switch" among other things. As such, the Office Action, yet again, has ignored these elements of the claims, including, among others, "when the interface control command introduces a security risk, determining a state of a switch." As such, Applicant requests a corresponding showing of where *Fisherman* describes "when the interface control command introduces a security risk, determining a state of a switch." Therefore, the Office Action fails to show how the cited portions of *Fisherman* teach each and every element as arranged in the claims.

Further, the Applicant cannot find where *Fisherman* at Col. 5, lines 7—11 teaches "determining whether the interface control command introduces a security risk," as previously described in the previous response and as discussed above. Finally, the citation to Cols. 5, 6 and 7 does not comply with requirements of 37 C.F.R. §1.104(c)(2) requiring that the Office Action show "the particular relied on must be designated as merely as practicable." As such, the Office Action continues to fail to show where *Fisherman* describes "determining whether the interface control command introduces a security risk."

According to the Office Action:

> *Fisherman* teaches an interface control command in Col. 4, lines 2-3. *Fisherman* also states that when the system is in the active state the commands are hidden and therefore cannot be executed by the CPU. This is synonymous to inhibiting the interface control command.

However, the Office Action does not cite to anywhere in *Fisherman* to support the proposition that "*Fisherman* also states that when the system is in the active state the commands are hidden and therefore cannot be executed by the CPU." As such, the Office Action fails to show where *Fisherman* describes "when the interface control command introduces a security risk, determining a state of a switch."

According to the Office Action on page 3 "Security risks as taught by [SIC] are commands that can cause potential damage to the system" and "[t]hese commands must only be executed from authorized program entities." The Examiner relies on the specification of *Fisherman* in Cols. 5—7 for support of this interpretation. Unfortunately, the Office Action fails to show where *Fisherman* describes a security risk and as such Applicant requests a showing. Also, as previously stated, the Office Action fails to show where in Cols. 5—7 of *Fisherman* "when the interface control command introduces a security risk, determining a state of a switch" is specifically described. Further, the Office Action states "the system must be able to recognize individual commands if it is able to differentiate between potentially threatening commands and lesser important commands." However, the Office Action fails to show where *Fisherman* recognizes these individual commands or is able to differentiate between potentially threatening commands and lesser important commands. As a result, the assertions in the Office Action as shown above are conclusory and without support.

According to the final Office Action on page 4:

> [The] Examiner interprets a switch as a change between at least two states. Switches can be implemented in hardware or software. It is a fine line between hardware and software switches for the reason that eventually all software must be implemented at the hardware level. Certainly, a switch is not just a transistor. With that in mind, *Fisherman's* system has two states, an active state (protected) and a passive state (unprotected).

The Examiner provides no support for this assertion and as such, a showing is requested. The *Fisherman* language relied on for the above assertion at Col. 4, lines 26—32 that states "the reason for the use of the key program is that the PPSM 22 determines the type of program which is attempting to change the status, and the PPSM 22 allows a change in its status only if flags are present indicating that the key program is active," is limited to describing a change in status flags indicating that the key program is active rather than "when the interface control command

introduces a security risk, determining a state of a switch; then the state of the switch is in a protected state, inhibiting execution of the interface control command." On page 5 the final Office Action asserts that with regard to an "electrical switch" the Examiner cites the previous interpretation of a switch. However, nowhere does the Office Action show where *Fisherman* teaches "an electrical switch." The Office Action fails to show where *Fisherman* teaches "*Fisherman's* system has two states, an active state (protected) and a passive (unprotected)." Since the Office Action fails to show where *Fisherman* describes the language as asserted, the assertion in the Office Action is conclusory and without support.

According to the final Office Action on page 4 at the last paragraph "*Fisherman* also states that when the system is in the active state the commands are hidden and therefore cannot be executed by the CPU." The Office Action further states "this is synonymous to inhibiting the interface control command." As previously stated, the cited portion of *Fisherman* at Col. 4, lines 2—3 merely teaches a control-command handler rather than inhibiting execution of the interface control command. Further, the assertion that when the system is in the active state the commands are hidden is synonymous to inhibiting the interface control command "and" is without support and therefore conclusory. Further, the Office Action fails to show where the control-command handler of *Fisherman* is inhibited, and therefore, the assertion in the Office Action is without merit.

According to the final Office Action on page 5 "which of these modules equates to the Claim 'protection engine' is really a moot point based on how one interprets a 'protection engine.'" However, the assertion in the Office Action that the claimed "protection engine" is really a moot point based on how one interprets a "protection engine" is unsupported, conclusory, utilizes circular reasoning and not in compliance with 37 C.F.R. §1.104(c)(2). The

assertion that "what really matters is that the elements of *Fisherman's* system function in a way that anticipates the claimed invention" is conclusory, unsupported and without merit. The final Office Action acknowledges that "while *Fisherman* does not come out and explicitly state that a format command is a high security risk, he does say that commands altering the boot sector of a hard disk are monitored." As such the Office Action acknowledges that *Fisherman* fails to teach "a format command is a high security risk." Again, the Office Action fails to show where *Fisherman* describes "receiving in a protection engine, an interface control command" and "determining whether the interface control command introduces a security risk" as arranged in the claims. As such, the Office Action continues to ignore explicit elements in the claims and as a result fails to show how *Fisherman* describes each and every element as arranged in the claims.

The *Fisherman* language at Col. 9, lines 23—30 cited on page 3 states "In order to obtain free access to the hard disk 34, the CPU 64 must switch the PPSM 22 to the passive mode, and to do this, the CPU 64 must use one of the key programs" and "the reason for the use of the key program is that the PPSM 22 determines the type of program which is attempting to change the status, and the PPSM 22 allows a change in the status only if the flags are present indicating that the key program is active" is limited to determining the type of program that is attempting to change the status rather than "determining whether the interface control command introduces a security risk." Applicant would like to point out the distinction between where the PPSM 22 determines the type of program that is attempting to change the status and "determining whether the interface control command introduces a security risk." Applicant would also like to point out that the cited portion of *Fisherman* fails to disclose "a security risk," let alone determine whether the interface control command introduces a security risk. Accordingly, a corresponding showing

is requested. As such, at least for these reasons the Office Action has ignored at least these and other elements of the claims.

The *Fisherman* language cited in the Office Action that states "the second memory 68 which is always accessible to the CPU 64, stores the set of key programs which are used to change the status of the PPSM 22" (*Fisherman* Col. 4, lines 37–40) and "the programmable controller 70 prevents access to the hard disk 34 and forbids access to the first memory 66" (*Fisherman* Col. 4, lines 40–42) is limited to a second memory 68 to store the set of key programs that are used to change the status of the PPSM and a controller 70 that prevents access to the hard disk 34 and forbids access to the first memory 66" rather than "when the state of the switch is a protective state, inhibiting execution of the interface control command." Applicant would like to point out the distinction between a second memory 68 and a programmable controller 70 that prevents access to the hard disk 34 and forbids access to the first memory 66 and "when the state of the switch is a protective state, inhibiting execution of the interface control command." Applicant would like to point out that the cited portion of *Fisherman* fails to describe a switch, let alone "when the state of the switch is a protective state." Further, Applicant would like to point out the cited portion of *Fisherman* fails to describe an interface control command let alone "inhibiting execution of the interface control command" among other things. As such, the Office Action ignores multiple elements of the claims including among others "when the state of the switch is a protective state, inhibiting execution of the interface control command." As a result, the Office Action fails to show how, and Applicant requests a showing of how, *Fisherman* teaches each element of the claims *inter alia*, "when the state of the switch is a protective state, inhibiting execution of the interface control command."

The *Fisherman* language cited in the Office Action states "In the passive mode, the PPSM 22 permits the protection programs to be read and does not affect the access to the hard disk 34 by the CPU" and "In order to obtain free access to the hard disk 34 the CPU must switch the PPSM 22 to the passive mode" (*Fisherman* Col. 4, lines 20–24), and to do this the CPU 64 must use one of the key programs," which is limited to using a key program to switch the PPSM 22 to the passive mode, rather than "when the state of the switch is in an unprotected state, allowing execution of the interface control command." Applicant would like to point out the distinction between obtaining full access to the hard disk 34 "for which" the CPU must switch the PPSM 22 to the passive mode and "when the state of the switch is in an unprotected state, allowing execution of the interface control command." (*Fisherman* Col. 4, lines 20–24). Applicant would like to point out that the cited portion of *Fisherman* fails to teach or refer to a switch let alone "when the state of the switch is in an unprotected state." *Fisherman* merely recites that the CPU must switch the PPSM 22 to the passive mode, and to do this, the CPU 64 must use one of the key programs rather than "a switch" let alone "when the state of the switch is in an unprotected state." Applicant would like to point out the distinction between a key program and a switch. As such, the Office Action ignores yet another limitation in the claims, and as a result Applicant requests a corresponding showing. Consequently, the Office Action fails to show how *Fisherman*, as cited, teaches each and every element of the claims, namely "when the state of the switch is in an unprotective state, allowing execution of the interface control command."

Independent Claim 33

The *Fisherman* language cited in the Office Action at ¶14, lines 16–19 states that the protection command handler 48 checks the access privilege of the calling program by comparing the code of the incoming command with the protection control command set, which is unique to

each HDPS 20 which, in turn, is limited to checking the access privilege of a calling program rather than "when the interface control command introduces a security risk, determining whether a source of the interface control command is authentic." Applicant would like to point out the distinction between checking the access privilege of the calling program and determining "when the interface control command introduces a security risk." Further, the cited portion of *Fisherman* fails to describe a "security risk" let alone "when the interface control command introduces a security risk."

The cited portion of *Fisherman* describes checking the access privilege of a calling program rather than "determining whether a source of the interface control command is authentic." As such, the Applicant respectfully requests a showing. For at least the reasons stated above, *Fisherman*, as cited, fails to teach each and every element of the claims, namely "when the interface control command introduces a security risk determining whether a source of the interface control command is authentic."

The cited portion of *Fisherman that* states "If the code of the incoming command does not match the current protection control command set, then the command is not executed, the system log records an attempt at unsanctioned access to the command handler 48, and an error code is generated in the corresponding registers, and control is returned to the key program 54" is limited to determining if an incoming command does not match the current protection control command set and generating an error code, rather than "when the source of the interface control command is not authentic, inhibiting execution of the interface control command." (*Fisherman*, Col. 14, lines 19–24) Applicant would like to point out the distinction between "the incoming command data" and "the interface control command." Further, the cited portion of *Fisherman* fails to describe any such type of interface command.

Dependent Claims 2 and 34

Applicant repeats the relevant remarks made above. Applicant further argues that these claims contain novel and non-obvious elements not contained in their respective independent claims. Applicant respectfully repeats the relevant comments above. For the reasons stated above, since the cited portions of *Fisherman* fail to teach "an interface control command" *Fisherman* fails in "providing an indication that the execution of the interface control command was inhibited."

Dependent Claims 3, 4, 5, 6 and 7

Applicant repeats the relevant remarks made above. Applicant further argues that these claims contain novel and non-obvious elements not contained in their respective independent claims. The *Fisherman* language as cited in the Office Action that states "the initial key program 52 returns control to the Post Procedure, at which time the PPSM 22 is switched to the active mode" is limited to a PPSM 22 (Protection-Programs Support Module) and is switched to the active mode (*Fisherman* Col. 11, lines 51–53), rather than "changing the state of the switch to the protected state when a timeout duration has elapsed." The Applicant would like to point out the distinction between the PPSM 22 and a switch. If the Examiner equates the PPSM 22 to the switch, then the Office Action has failed to show where *Fisherman* describes a protection engine. As such, the Office Action ignores yet another element of the claims.

With respect to Claim 4, the cited portion of *Fisherman* at Col.14, lines 30–35 that states "If the activity of the protection control program 50 is confirmed, then the requested protection control command is executed" and "After the execution of the requested protection control command, control returns to the key program 54 of the protection control command handler, upon which the PPSM 20 is switched to the active operating mode" is limited to determining the

activity of the protection control program rather than "when the execution of the interface control command has been completed, changing the state of the switch to the protected state."

The Office Action fails to show where *Fisherman* describes "determining when the execution of the interface control command has been completed." Applicant repeats the above relevant remarks including those with respect to the switch limitation as claimed. Since the cited portion of *Fisherman* merely describes switching the key program 54 to the active operating mode, *Fisherman* fails to describe "when the execution of the interface control command has been completed, changing the state of the switch to the protected state."

With regard to Claim 5, the cited portion of *Fisherman* at Col. 4, lines 29–30 states "After the PPSM 22 is switched to the passive mode, the key program transfers control to the protection programs stored in the PPSM 22" rather than "determining the state of an electrical switch (physical switch)." The Applicant would like to point out the distinction between the PPSM 22 and "an electrical switch (physical switch)." According to the Office Action dated May 13, 2004, "It is a fine line between hardware and software switches for the reason that eventually all software must be implemented at the hardware level." However, this assertion does not explain how the cited portion of *Fisherman* describes "an electrical switch (physical switch) and therefore is conclusory." The cited portion of *Fisherman* fails to describe a switch, let alone "an electrical switch (physical switch) because *Fisherman*, as cited, merely describes a protection program support module PPSM 22. As such, the Office Action has ignored yet another element of the claims, namely "an electrical switch (physical switch)." Applicant request showing of: "an electrical switch (physical switch)."

As per Claim 6, the cited portion of *Fisherman* at ¶4, lines 38–42 states "the second memory 68, which is always accessible to the CPU 64 stores the set of key programs which are

used to change the status of the PPSM 22" is limited to a key program used to change the status of the PPSM 22 rather than "determining the state of a software-based switch." According to the assertion in the Office Action, the Office Action ignores the distinction between claims 5 and 6. Applicant requests a showing of "determining the state of a software-based switch."

With regard to Claim 7, the cited portion of *Fisherman* at ¶4, lines 25–30, states "The reason for the use of the key programs is that the PPSM 22 determines the type of program which is attempting to change the status, and the PPSM 22 allows a change in the status only if the flags are present indicating that the key program is active" rather than "using cryptographic techniques to determine the state of the software-based switch." The Applicant would like to point out the distinction between allowing a change in the status only if flags are present indicating that the key program is active and "using cryptographic techniques to determine the state of the software-based switch." For example, the Applicant would like to point out the distinction between determining if the key program is active and using cryptographic techniques. The cited portion of *Fisherman* fails to describe cryptographic techniques, let alone "using cryptographic techniques to determine the state of the software-based switch." As such, the Office Action yet again ignores a limitation in the claims.

Dependent Claims 8, 9, 10, 11, 12, 27, 35, 36, 37, 38, 39 and 53

Applicant repeats the relevant remarks made above. Applicant further argues that these claims contain novel and non-obvious elements not contained in their respective independent claims.

Claims 19, 20, 21, 24, 45, 46, 47 and 50

The Office Action on page 6 cites ¶5, lines 7–10, which states "During the protection process, each logical drive of the MS-DOS operating system 28 is interpreted by the HDPS 20 as a fixed set of zones of the disk space, with different access rules for each zone" which is limited

to describing a fixed set of zones rather than "determining whether the interface control command is a hard disk drive formatting command" as recited in Claims 19 and 45. Applicant would like to point out the distinction between a fixed set of zones of the disk space and "an interface control command is a hard disk drive formatting command." The *Fisherman* language cited at ¶5, lines 30–35, which states "the fourth zone called the Clust Zone occupies the disk space from the first sector of the first cluster of the disk to the beginning of the next zone, which is described below" and "Access to this zone is permitted for reading and writing" and "before writing operations, the proposed changes are analyzed in order to prevent unsanctioned changes in the protected files and directories" is limited to reading and writing rather than "determining whether the interface control command is a hard disk drive formatting command." Applicant would like to point out the distinction between reading and writing and "determining whether the interface control command is a hard disk drive formatting command." As such, the Office Action ignores yet another element of the claims. Further, the dependent claims contain novel and non-obvious elements not contained in their respective independent claims. Accordingly, Applicant respectfully requests a corresponding showing for each claim.

Dependent Claim 59

The Office Action on page 7 cites *Fisherman* ¶14, lines 10–15, which states "Access to the HDPS command handler 48 is made by a call of the key program 54 of the protection command handler 48" and "When the key program 54 of the protection control command handler 48 is executed, the PPSM 20 is switched to the passive mode and the protection control command handler 48 is called" is limited to "switching the PPSM 20 to the passive mode when the key program 54 of the protection command handler 48 is executed" rather than "issuing a challenge to the source of the interface control command." Applicant would like to point out the distinction between merely executing the control command handler and "issuing a challenge to

the source of the interface control command." Applicant repeats the relevant remarks above and would like to point out that the cited portion of *Fisherman* fails to describe an interface control command, let alone "issuing a challenge to the source of the interface control command." Further, Applicant would like to point out that the cited portion of *Fisherman* appears not to describe "issuing a challenge," let alone "issuing a challenge to the source of the interface control command." For these and the above reasons, the Office Action ignores yet another element of claims.

Claims 60, 61, 65, 66, 67, 68 and 69

With respect to claims 60, 65, 66, 67, 68 and 69, the Office Action on page 7 cites *Fisherman* ¶1, lines 63–66, which states "the control device also reads the signatures of all the protected files and compares the signatures of the loaded files with the reference signatures" which is limited to comparing the signatures of the loaded files with the reference signatures rather than "comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system." The Applicant would like to point out the distinction between reading the signatures of all the protected files and comparing the signatures of a loaded file with reference signatures and "comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system." Applicant cannot find where the cited portion of *Fisherman* describes "a mathematical function of a value accessible only to the protection engine and to the operating system, let alone "comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system."

As per Claim 61, the Office Action on page 7 cites *Fisherman* at ¶1, lines 45–55, which states "a typical example of a protection subsystem developed and patented by Imperacle Research Systems Incorporated (citation omitted) can be accessed by the operating system for

modifications only during installation" and "the hardware for this subsystem includes programmable external memory and a programmable external control device" is limited to a subsystem that can be accessed by the operating system for modifications only during installation rather than "writing the value from a processor to a one-time writable register in the protection engine (by an operating system) during a boot process (before application software is enabled)." Applicant would like to point out the distinction between a subsystem that can be accessed by the operating system for modifications only during installation and "writing the value from a processor to a one-time writable register in the protection engine (by an operating system) during a boot process (before application software is enabled)." Applicant would like to point out that the cited portion of *Fisherman* states that "the subsystem can be accessed by the operating system for modifications only during installation" which fails to describe a one-time writable register for a boot process, let alone "writing the value from a processor to a one-time writable register in the protection engine (by an operating system) during a boot process (before application software is enabled)." As such, the Office Action ignores yet another element of the claims, namely "writing the value from a processor to a one-time writable register in the protection engine (by an operating system) during a boot process (before application software is enabled)."

Independent Claim 64

Applicant respectfully repeats the relevant remarks made above. The Office Action appears to equate the protection engine to the PPSM 22 by referring to Fig. 1 when discussing the protection engine. However, the Office Action cites *Fisherman* ¶4, lines 29–30 to describe the switch and, as previously stated, this cited portion of *Fisherman* appears to refer to the switch as the PPSM 22. Accordingly, the Office Action, in contradictory fashion, requires that the PPSM 22 describe both the protection engine and the switch where these two elements are

described as separate elements in the claim. As such, the Office Action yet again ignores a element of the claims. Claims 64 through 69 further recite other novel and nonobvious elements not described in Claim 1. With regard to Claim 65, Applicant repeats its remarks above, including those with regard to Claim 3 above. Further, the Office Action on page 8 recites *Fisherman* ¶11 lines 50–53, which states "the initial key program 52 returns control to the Post Procedure, at which time the PPSM 22 is switched to the active mode," which is limited to switching the PPSM 22 to the active mode rather than "a timer operatively coupled to the switch to reset the switch to the protected state after a period of time has elapsed." Applicant would like to point out the distinction between a timer and switching the PPSM 22. Further, Applicant cannot find where the cited portion of *Fisherman* describes a timer, let alone "a timer operatively coupled to the switch to reset the switch to the protected state after a period of time has elapsed."

With regard to Claim 66, the Office Action on page 6 cites ¶14 lines 30–35, which, as previously cited with respect to Claim 4, is limited to switching the PPSM 20 to the active operating mode after execution of the requested protection control command rather than "an interface control command execution completion sensor operatively coupled to the switch to reset the switch to the protected state after an execution of the interface control command has been completed." Applicant would like to point out the distinction between "an interface control command execution completion sensor" and the PPSM 20.

Independent Claims 67, 68 and 69

The Applicant respectfully repeats the above-relevant remarks. As stated above, among other things, the Office Action fails to show "a protection engine operatively coupled to the interface controller for preventing unauthorized access to the interface device and operatively coupled to receive the interface control command to determine whether a source of the interface control command is authentic and to selectively allow or inhibit execution of the interface

control command by the interface controller, depending on whether or not the source of the interface control command is authentic."

With respect to Claims 68 and 69, these claims add additional novel and non-obvious elements not recited in Independent Claim 67. Further, Applicant respectfully repeats the relevant remarks made above.

Claim Rejections Under 35 U.S.C. § 103

It is well established that, to establish *prima facie* obviousness, all the claim limitations must be taught or suggested by the prior art. In addition, there must be some teaching, motivation or suggestion that either the prior art or the references themselves can make the combination and modifications as asserted in the Office Action.

"Measuring a claimed invention against the standard established in §103 requires the difficult but critical step of casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references in the then-accepted wisdom in the field.[3] Close adherence to this methodology is especially important where the very ease with which the invention can be understood may prompt one "to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher."[4]

Claims 13–17, 28–32, 40–44 and 54–58 are rejected under 35 U.S.C. § 103(a), based on *Fisherman* in view of Glossary of Information Technology Acronyms and Terms. The Office Action acknowledges that *Fisherman* "is silent in disclosing and allowing data to be written to a

[3] W.L. Gore & Assoc., Inc. v. Garlock, Inc., 721 F.2d 1540, 1553, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

[4] *Id.*

parallel port, serial port, USB port, and an IEEE-1394 port" and that *Fisherman* does not teach "a computer system which controls data access to the system's basic input/output system."

The Office Action appears to assert that one skilled in the art while viewing *Fisherman* would somehow be directed to reading the various ports as defined in the Glossary of Information Technology Acronyms and Terms ("GITAT"). However, the Office Action fails to show how one reading *Fisherman* would somehow be motivated to think of viewing such a Glossary in order to modify *Fisherman* to include these various ports. Further, *Fisherman* repeatedly describes the invention being directed to protecting information on a local area network ("LAN") in ¶1 lines 15–37 and, as such, has no need for addressing the possibility that "an unauthorized person might try to send sensitive data via an outlet port." Therefore, the Office Action fails to show sufficient motivation for one skilled in the art to modify *Fisherman* as asserted. Furthermore, the Office Action fails to show how one skilled in the art reviewing *Fisherman* vis à vis to a "personal computer hard disk protection system" would suddenly be motivated to refer to the Glossary of Information Technology, which is not specifically related to a "personal computer hard disk protection system."

Claims 18, 25, 26, 51 and 52 are rejected under 35 U.S.C. § 103(a) based on *Fisherman*, GITAT, and further in view of *Davis* (United States Patent 6,025,547). The Office Action acknowledges that *Fisherman* fails to teach control and commands sent to the thermal management controller.

The Office Action, on page 12 reference no. 4, cites *Davis* ¶6, lines 9–16, which states "A system management controller is, in accordance with the invention they provide, an operating system independent mechanism to regulate (manage, monitor, and control) a computer system", "That is, SMC 102 is capable of regulating computer system before power on self-test ("POST")

procedures as well as before, during and after operating system load ("BOOT") operations" and "another benefit of a system management controller in accordance with the invention is that the management mechanism may be invoked remotely" is limited to merely an operating system independent mechanism to manage, monitor and control a computer system rather than "any form of personal computer hard disk protection system." Since *Fisherman* is directed to a personal computer hard disk protection system and *Davis* is directed to a management controller, one skilled in the art would not be motivated to modify *Fisherman's* personal computer hard disk protection system to include the thermal management controller allegedly described in *Davis*. Since these are in completely different endeavors of art, one skilled in the art would not be motivated to make such a modification to *Fisherman*.[5]

As per Claims 62—63, the Office Action acknowledges that *Fisherman* is silent "in expressly disclosing performing a mathematical operation in the challenge to produce a correct response value." Nevertheless, Applicant respectfully repeats the relevant remarks made above. Applicant requests a showing of where the reference to teach "in expressly disclosing performing a mathematical operation in the challenge to produce a correct response value." Applicant further argues that these claims contain novel and non-obvious elements not contained in their respective independent claims.

New Claim 71

Applicant repeats the relevant marks made above, especially those with respect to where *Fisherman* fails to teach "an interface control command." Applicant is unable to find where

[5] Wang Laboratories, Inc. v. Toshiba Corp., 993 F.2d 858, 26 U.S.P.Q.2d 1767 (Fed. Cir. 1993) (Patent Claims were directed to single inline memory modules (SIMMs) for installation on a printed circuit motherboard for use in personal computers. Reference to a SIMM for an industrial controller was not necessarily in the same field of endeavor as the claimed subject matter merely because it related to memory). *See* MPEP §2141.01(a).

Fisherman as cited teaches "a security risk determined from at least one of: a type of interface control command, an area of memory affected by the interface control command, a device affected by the interface control command, data associated with the interface control command, an operand associated with the interface control command, and a relationship of the interface control command to other interface control command." *Fisherman* fails to teach each and every element as arranged in claim 71.

Dependent Claims 71, 72 and 73

Applicant repeats the relevant remarks made above, especially those arguments arguing the distinction between limitations of a physical switch, a hardware-based switch and a software-based switch. For the reasons stated above, since the cited portions of *Fisherman* fail to teach either a hardware or software-based switch, Fisherman fails to teach each and every element as arranged in the claims. Applicant further argues that these claims teach novel and nonobvious elements not contained in claim 70.

Consequently, the Office Action has ignored numerous elements of the claims, as described above. As a result, combinations of the cited references, including *Fisherman*, lack the advantages of the claimed invention. Therefore, the alleged reference-by-reference and limitation-by-limitation analysis, fail to demonstrate how *Fisherman* or the combination of *Fisherman* with the other cited references teach each and every claimed element as arranged in the claims.

CONCLUSION

Accordingly, Applicant respectfully submits that the Claims are in condition for allowance, and that an early Notice of Allowance be issued in this application. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance prosecution of this application.

Respectfully submitted,

By: Themi Anagnos
Themi Anagnos
Registration No. 47,388

Date: September 10, 2004

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7500
FAX: (312) 609-5005